Marlene H. Dortch, Secretary
Federal Communications Commission
Office of the Secretary
445 12th Street, SW
Room TW-B204
Washington, DC 20554

Re: Comments in Support of Petitions to Reconsider Action in Rulemaking Proceeding, WC Docket No. 16-106, the ISP Privacy Rule

Dear Secretary Dortch,

The American Legislative Exchange Council (ALEC) writes in support of various petitions for reconsideration filed with the Federal Communications Commission and relating to WC Docket No. Number 16-106, or the so-called ISP Privacy Rule (hereafter "the Rule"). Our position is based on a number of factors, including the degree to which the Privacy Rule pre-empts state regulations and the likelihood the Rule would not achieve its stated end of protecting consumer privacy.

Introduction

ALEC is the nation's largest, voluntary membership association for state legislators, with 25 percent of all state legislators as members. Over 70 Representatives and 13 United States Senators are among our alumni.[1] Consistent with our mission,[2] we seek to advance the Jeffersonian principles of Federalism, Free Markets, and Limited Government through policy discussions, education of policy makers in various subjects including Communications and Technology, and the adoption of model policy.

The concept of federalism, as embodied in the 10th Amendment to the United States Constitution, demands the federal government recognize states as its equal governing sovereigns. The Supreme Court and various federal circuit courts of appeal have repeatedly held that when a federal agency seeks to preempt state laws, the agency must have a clear statement of authority from Congress.[3]

Furthermore, the concept of federalism demands that the federal government recognize states are often better able to protect the interests of their citizens than the federal government.

---

[1] See https://www.alec.org/about/alumni/

[2] "The American Legislative Exchange Council (ALEC) is a 501(c)(3) nonprofit organization dedicated to advancing and promoting the Jeffersonian principles of limited government, free markets and federalism at the state level. ALEC accomplishes this mission by educating elected officials on making sound policy and providing them with a platform for collaboration with other elected officials and business leaders." *See generally*, https://www.alec.org/about/.

[3] *See, e.g., Nixon v. Missouri Municipal League*, 541 U.S. 125 (2004) and *State of Tennessee v. Federal Communications Commission*, ___ F.3d ____ (6th Cir. 2016).

The FCC Should Grant the Petitions for Reconsideration to Clarify the Extent to Which the Rule Preempts State Privacy Standards

The Rule preempts state regulation of Internet privacy.

> In this section, we adopt the proposal in the NPRM and announce our intent to preempt state privacy laws, including data security and data breach laws, only to the extent that they are inconsistent with any rules adopted by the Commission.[4]

The relevant section, at paragraphs 324 through 331, continues to discuss the FCC's opinions regarding preemption.

At no time in the discussion does the FCC directly address the impact on states. Instead, the FCC speculates, issues broad statements indicating intent to create a privacy standard baseline, then promises a case-by-case analysis. Nor does the FCC ever address the concerns raised in comments filed on the rule by 16 attorneys general.

> We are concerned about the possible preemption of state laws. Although the [NPRM] recognizes that 'states are very active participants in ensuring their citizens have robust privacy and data security protections,' the proposed rule may unwittingly preempt important state initiatives… It is of paramount importance that any federal regulations not impair states' ability vigorously to protect their citizens as they deem appropriate.[5]

Some states have strict standards for ISPs. Some states place minimal burdens on ISPs. Still other states do not place additional burdens on ISPs. Minnesota, for example, prohibits ISPs from disclosing a customer's data,[6] including online browsing history,[7] without the customer's authorization. Utah, similarly, requires a company, whether an ISP or other "commercial entity," to disclose whether it intends to selling a customer's data.[8] Though the law requires disclosure, it is satisfied with a simple disclaimer, which "shall read substantially as follows: 'We may choose to disclose nonpublic personal information about you, the consumer, to a third party for compensation.'"[9]

Minnesota regulates ISP handling of personal information in a different manner than Utah. Minnesota requires an ISP to obtain a customer's authorization, while Utah merely requires disclosure. Both states have debated the topic of privacy, come to different conclusions on how to protect privacy, and have different enforcement mechanisms.

---

[4] Docket No. 16-106, FCC 16-148 at 324.
[5] Letter signed by 16 Attorneys General, previously filed with the FCC and *available at* http://src.bna.com/itA.
[6] Minnesota Statute § 325M.04. *See generally* Minnesota Statute §§ 325M.01, *et seq.*
[7] Minnesota Statute § 325M.01.
[8] Utah Code §§ 13-37-102, *et seq.*
[9] Utah Code § 13-37-201(3)(a).

Pursuant to the FCC's reasoning, the Rule may not preempt Minnesota's law, as the state's standards appear stricter than the FCC's standard. On the other hand, the Rule likely preempts Utah's law, as Utah's law does not require an opt-out provision.[10]

Prior to the Rule, states worked hand-in-hand with the Federal Trade Commission. The FTC assumed the role of the federal government's chief privacy enforcement agency since the 1970s.[11] The approach it developed over the course of the past few decades means that it has as deep knowledge regarding privacy enforcement and can respond to actual privacy breaches rather than prospective breaches.

The Rule interferes with the traditional enforcement, by creating an uncertain regulatory environment. Who enforces privacy standards: the FCC, the FTC, states, or a combination? Rather than permitting states and the FTC to examine alleged privacy breaches on a case-by-case basis, at the very least the Rule "places two privacy cops on the same Internet beat."[12]

States have a myriad of privacy standards. These standards reflect the concerns of states' citizens. They are a hallmark of federalism. The FCC did not properly address federalism concerns in the Rule or the extent to which the Rule would actually preempt state standards. Reconsidering the Rule will allow the FCC to reexamine the role of states and the FTC in protecting consumer privacy.

The FCC Should Grant the Petitions for Reconsideration because the Rule Assumes ISPs Currently Use Technology Pervasive in 1990s and because the Rule Fails to Protect Consumer Data

The Rule properly identified the critical nature of privacy. "Privacy rights are fundamental because they protect important personal interests—freedom from identity theft, financial loss, or other economic harms, as well as concerns that intimate, personal details could become the grist for the mills of public embarrassment or harassment or the basis for opaque, but harmful judgments, including discrimination."[13] The Rule, though, fails to account for the role ISPs actually play compared to edge service providers and fails to consider how technology works.

For example, the largest telecommunications privacy breach happened to Securus Technologies, according to comments filed by the Technology Policy Institute.[14] Securus is not an ISP. It is a specialty telecommunications company, providing telephone services to prisons. The privacy breach experienced by Securus impacted an estimated 70 million records.

---

[10] Docket No. 16-106, FCC 16-148 at 324-331.
[11] "Protecting Consumer Privacy", FTC, available at, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy.
[12] Leibowitz, Jon and Jonathan Neuchterlein, *The New Privacy Cop Patrolling the Internet*, Fortune, May 10, 2016, *available at* fortune.com/2016/05/10/fcc-internet-privacy/.
[13] Docket No. 16-106, FCC 16-148 at 1.
[14] Lenard, Thomas and Scott Wallsten, *An Economic Analysis of the FCC's Privacy Notice of Proposed Rulemaking*, Technology Policy Institute, May 2016. *Available at* https://techpolicyinstitute.org/wp-content/uploads/2016/05/Lenard_Wallsten_FCCprivacycomments.pdf.

The report continues, identifying the largest ISP privacy breach. According to the authors, that breach impacted Verizon Enterprise Services with an estimated 3 million records exposed. Compare that to recent breaches, whether of Target, the Office of Personnel Management, or Yahoo. The Yahoo breach alone impacted an estimated one billion users.

The Rule paints the picture that ISPs have access to a broad cross-section of data and that they can connect this data to specific consumers. This assumption simply does not comport with practice, unless the FCC considers practices from a decade ago relevant. Ten years ago, consumers browsed the Internet primarily from desktop PCs. Consumers accessed the Internet through landline telephone or cable wires. DSL was still a relatively new technology. During this time, ISPs provided both last mile service and DNS lookup services, and Internet traffic was largely unencrypted.

Today, consumers access the Internet from a plethora of electronic devices, including mobile phones, laptops, and tablets. They connect these devices in different ways at different locations. They may work from the WiFi at a coffee shop, connect through a mobile broadband connection, or even connect from their homes.

ISPs no longer handle DNS lookup services and contemporary enhanced encryption practices ensure that information once visible to ISPs is inaccessible.

According to researchers at Georgia Tech,

> "[T]he recent and rapid shift to HTTPS and other forms of encryption is perhaps the clearest and simplest way to explain why ISPs today and in the future do not have 'comprehensive' access to users' Internet activities. HTTPS blocks the possibility of ISP access to the content of users' activities – the technology called 'deep packet inspection' does not work on encrypted communications. HTTPS also blocks the possibility of ISP access to detailed URLs, which can reveal granular details of a user's search or other online activities.[15]

Advancements in technology mean that ISPs have access to precious little consumer data. They certainly have access to far less than the FCC's aversion that providers "have access to vast amounts of information about their customers including when we are online, where we are physically located

[15] Swire, Peter, Justin Hemmings and Alana Kirkland, *Online Privacy and ISPS: ISP Access to Consumer Data is Limited and Often Less than Access By Others*, The Institute for Information Security & Privacy at Georgia Tech, February 29, 2016, *available at* www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf. The volume of encrypted Internet traffic has jumped exponentially over the past couple years. In 2014, an estimated 35 percent of Internet traffic was encrypted. After Netflix transitioned to HTTPS in 2015, the percentage of encrypted traffic jumped from 35 percent to 65 percent. Other experts estimate that 70 percent of Internet traffic transitioned to some form of encrypted traffic by the end of last year. *See, e.g.*, "Encrypted Internet Traffic", Sandvine, May 8, 2015, available at https://www.sandvine.com/downloads/general/global-internet-phenomena/2015/encrypted-internet-traffic.pdf and Mario Trujillo, *Study finds about half of Web traffic is encrypted*, The Hill, February 29, 2016, available at http://thehill.com/policy/technology/271152-study-finds-about-half-of-web-traffic-is-encrypted.

when we are online, how long we stay online, what devices we use to access the Internet, what websites we visit, and what applications we use."[16]

If yesteryear's practices existed today, perhaps the FCC would have a legitimate concern. Advancements in technology and ISP practices neuters the FCC's justification of the Rule and perhaps belies the Rule's true intent: providing a competitive advantage to certain edge service providers.[17]

Conclusion

The American Legislative Exchange Council supports the petitions for reconsideration of the Rule. Reconsidering the Rule will permit the FCC to examine salient issues it ignored when it first promulgated the Rule, including the roles of the FTC and the states in protecting consumer data. It will also afford an opportunity to address whether modern technology has already addressed many of the concerns raised by the FCC.

Respectfully submitted this 6th day of March, 2017,

/s/
Jonathon Paul Hauenschild, Esq.
Director, Task Force on Communications and Technology
American Legislative Exchange Council
jhauenschild@alec.org

[16] Docket No. 16-106, FCC 16-148 at 2. The quantity and quality of data available to ISPs pales in comparison to the data available to edge service providers. Google, for example, has access to consumers' names and Internet search and browsing habits, at the least, if consumers have Gmail accounts. If consumers use Android smartphones, store documents on Google drive, link financial account information through Google Pay, or subscribe to a number of other Google services, the volume of personal information in Google's hands alone vastly exceeds the information ISPs can collect.

[17] *See above*, n. 12. Article by former FTC Chairman John Leibowitz and FTC General Counsel Jonathan Nuechterlein. Mr. Nuechterlein also previously served as Deputy General Counsel for the FCC. The authors suggest that the Rule will do nothing to protect consumer privacy, but will instead insulate big data from ISP competition.

> "Ironically, the proposed rules would do very little to promote the cause of 'privacy' in the first place. If they are adopted, all other participants in the Internet ecosystem will remain exempt, will continue collecting all of the same information that the ISPs would have collected, and may continue selling the same information as before to the same data brokers. The Big Data marketplace will carry on—except, ironically, the FCC will have insulated its largest players from ISP competition."